Cyber Law Consulting

TEXT BOOK OF CYBER CRIME AND PENALTIES [AS PER ITA A 2008 AND IPC] (Draft Version)

By Prashant Mali

www.cyberlawconsulting.com

INDEX

INTRODUCTION TO CYBER CRIME

Ch. 1.0 ANCIENT CYBER CRIME 05

Ch. 2.0 CRIMES INVOLVING MONEY 06

Ch. 3.0 CYBER PORNOGRAPHY & CHILD PORNOGRAPHY.....08

Ch.4.0 CYBER BULLYING.....15

Ch.5.0 IDENTITY THEFT 16

Ch.6.0 SALE OF ILLEGAL ARTICLES ON INTERNET 19

Ch.7.0 ONLINE GAMBLING 21

Ch.8.0 INTELLECTUAL PROPERTY CRIMES 24

Ch.9.0 EMAIL SPOOFING 27

Ch.10.0 FORGERY 30

Ch.11.0 CYBER DEFAMATION……33

Ch.12.0 CYBER STALKING ……35

Ch.13.0 WEB DEFACEMENT …… 38

Ch.14.0 EMAIL BOMBING …….... 41

Ch.15.0 DATA DIDDLING …… 43

Ch.16.0 SALAMI ATTACKS …….. 45

Ch.17.0 DENIAL OF SERVICE ATTACK (DoS & DDoS)……..... 46

Ch.18.0 VIRUS / WORM ATTACKS ,SPREADING OF CONTAMINATIO..... 49

Ch.19.0 TROJANS AND KEY LOGGERS……52

Ch.20.0 INTERNET TIME THEFT…… 56

Ch.21.0 WEB JACKING……..... 59

Ch.22.0 EMAIL FRAUDS ……..... 62

Ch.23.0 CYBER TERRORISM …… 65

TABLE OF SECTIONS..... 70

GLOSSARY 71

INTRODUCTION TO CYBER CRIME

What is a cyber crime?

Cyber crime is a generic term that refers to all criminal activities done using the medium of computers, the internet, cyber space and the worldwide web.

There isn't really a fixed definition for cyber crime. The Indian Law has not given any definition to the term ‘cyber crime'. In fact, the Indian Penal Code does not use the term ‘cyber crime' at any point even after its amendment by the Information Technology Act 2008 the Indian Cyber law. but "Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

What is Cyber law?

Cyber law (also referred to as Cyber law) is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world to human activity on the Internet. In India Information Technology Act [Amend.] 2008 is known as the Cyber law. It has a separate chapter XI entitled “Offences” in which various cyber crimes have been declared as penal offences punishable with imprisonment and fine.

Jurisdiction and sovereignty

Issues of jurisdiction and sovereignty have quickly come to the fore in the era of the Internet. The Internet does not tend to make geographical and jurisdictional boundaries clear, but Internet users remain in physical jurisdictions and are subject to laws independent of their presence on the Internet. As such, a single transaction may involve the laws of at least three jurisdictions:

1) the laws of the state/nation in which the user resides,

2) the laws of the state/nation that apply where the server hosting the transaction is located, and

3) the laws of the state/nation which apply to the person or business with whom the transaction takes place. So a user in one of the states in USA conducting a transaction with another user in Australia through a server in Chennai could theoretically be subject to the laws of all three countries as they relate to the transaction at hand.

Jurisdiction is an aspect of state sovereignty and it refers to judicial, legislative and administrative competence. Although jurisdiction is an aspect of sovereignty, it is not coextensive with it. The laws of a nation may have extra-territorial impact extending the jurisdiction beyond the sovereign and territorial limits of that nation. This is particularly problematic as the medium of the Internet does not explicitly recognize sovereignty and territorial limitations. There is no uniform, international jurisdictional law of universal application

Cyber attacks and effects

Cyberspace is constantly under assault. Cyber spies, thieves, saboteurs, and thrill seekers break into computer systems, steal personal data and trade secrets, vandalize Web sites, disrupt service, sabotage data and systems, launch computer viruses and worms, conduct fraudulent transactions, and harass individuals and companies.

Ch. 1.0 ANCIENT CYBER CRIME

The first recorded cyber crime took place in the year 1820.

That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime!

Today, computers have come a long way with neural networks and nano - computing promising to turn every atom in a glass of water into a computer capable of performing a billion operations per second.

In a day and age when everything from microwave ovens and refrigerators to nuclear power plants are being run on computers, cyber crime has assumed rather sinister implications.

Cyber crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief. The abuse of computers has also given birth to a gamut of new age crimes such as hacking, web defacement, cyber stalking, web jacking etc.

A simple yet sturdy definition of cyber crime would be “unlawful acts wherein the computer is either a tool or a target or both”.

The term computer used in this definition does not only mean the conventional desktop or laptop computer. It includes Personal Digital Assistants (PDA), cell phones, sophisticated watches, cars and a host of gadgets.

Recent global cyber crime incidents like the targeted denial of service attacks on Estonia have heightened fears. Intelligence agencies are preparing against coordinated cyber attacks that could disrupt rail and air traffic controls, electricity distribution networks, stock markets, banking and insurance systems etc.

Unfortunately, it is not possible to calculate the true social and financial impact of cyber crime. This is because most crimes go unreported.

Ch. 2.0 CRIMES INVOLVING MONEY

Money is the most common motive behind all crime. The same is also true for cyber crime. Globally it is being observed that more and more cyber crimes are being committed for financial motives rather than for “revenge” or for “fun”.

With the tremendous increase in the use of internet and mobile banking, online share trading, dematerialization of shares and securities, this trend is likely to increase unabated.

Financial crimes include cyber cheating, credit card frauds, money laundering, hacking, accounting scams etc., into bank servers, computer manipulation.

Section 66D Punishments for cheating by personation by using computer resource (Inserted Vide ITA 2008)

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 415 of IPC for any kind of Cheating.

Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat".

Explanation- A dishonest concealment of facts is a deception within the meaning of this section.

Illustrations

(a) A, by falsely pretending to be in the Civil Service, intentionally deceives Z, and thus dishonestly induces Z to let him have on credit goods for which he does not mean to pay. A cheats.

Illustration 1

Rs. 2,50,000 were misappropriated from Bank of Baroda in India through falsification of computerized bank accounts.

Illustration 2

The Hyderabad police in India arrested an unemployed computer operator and his friend, a steward in a prominent five-star hotel, for stealing and misusing credit card numbers belonging to hotel customers.

The steward noted down the various details of the credit cards, which were handed by clients of the hotel for paying their bills. Then, he passed all the details to his computer operator friend who used the details to make online purchases on various websites.

Illustration 3

In 2004, the US Secret Service investigated and shut down an online organization that trafficked in around 1.7 million stolen credit cards and stolen identity information and documents.

This high-profile case, known as "Operation Firewall," focused on a criminal organization of some 4,000 members whose Web site functioned as a hub for identity theft activity.

Illustration 4

In 2003, a hacker was convicted in the USA for causing losses of almost $25 million. The defendant pleaded guilty to numerous charges of conspiracy, computer intrusion, computer fraud, credit card fraud, wire fraud, and extortion.

The hacker and his accomplices from Russia had stolen usernames, passwords, credit card information, and other financial data by hacking into computers of US citizens. They would then extort money from those victims with the threat of deleting their data and destroying their computer systems.

Case of Extortion of Money through Internet

The complainant has received a threatening email and demanded protection from unknown person claiming to be the member of Halala Gang, Dubai. Police registered a case u/s. 384/506/511 IPC.

The sender of the email used the email ID xyz@yahoo.com & abc@yahoo.com and signed as Chengez Babar.

The Cyber cafes from which the emails has been made were monitored and the accused person was nabbed red handed.

Ch.3.0 CYBER PORNOGRAPHY & CHILD PORNOGRAPHY

Cyber pornography is believed to be one of the largest businesses on the Internet today. The millions of pornographic websites that flourish on the Internet are testimony to this. While pornography per se is not illegal in many countries, child pornography is strictly illegal in most nations today.

Cyber pornography covers pornographic websites, pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc).

Section 67: **Punishment for publishing or transmitting obscene material in electronic form (Amended vide ITAA 2008)**

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on **first conviction** with imprisonment of either description for a term which may extend to **two three** years and with fine which may extend to **five lakh rupees** and in the event of a **second or subsequent** conviction with imprisonment of either description for a term which may extend to **five years** and also with fine which may extend to **ten lakh rupee**s.

The Indian Penal Code, 1860 section 293 also specifies, in clear terms, the law against Sale etc. of obscene objects to minors. As per the IPC Act,

As per IPC, 1860, Section 292 - For the purposes of sub-section (2), a book, pamphlet, paper, writing, drawing, painting representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.]

Illustration 1

In the first case of this kind, the Delhi Police Cyber Crime Cell registered a case under section 67 of the IT act, 2000. A student of the Air Force Balbharati School, New Delhi, was teased by all his classmates for having a pockmarked face, used a free hosting provider to create www.amazing-gents.8m.net.

He regularly uploaded "morphed" photographs of teachers and girls from his school onto the website. He was arrested when the father of one of the victims reported the case to the police.

Illustration 2

The CEO of online auction website bazee.com (a part of the ebay group) was arrested by the Delhi police for violating India's strict laws on cyber pornography. An engineering student was using the bazee website to sell a video depicting two school students having sexual intercourse. Bazee.com was held liable for distributing porn and hence the CEO was arrested.

Illustration 3

The CEO of a software company in Pune (India) was arrested for sending highly obscene emails to a former employee.

Child pornography: The newly inserted section 67 B of ITAA, 2008deals with child pornography. The wordings of the section are very hard worded and makes even the recording in electronic form of any sexually explicit act with children shall be punishable under this section. Even if one is found to be engaged in online relationship with sexual overtone that may offend a reasonable adult on the computer resource would be punishable under this section. The expression "May offend a reasonable adult" is subject to judicial scrutiny and interpretation and leaves scope for misuse and controversy.

67 B Punishments for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form. Whoever,-

(a) Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.

Section 293 - " Sale, etc. of obscene objects to young persons - Whoever sells, lets to hire, distributes, exhibits or circulates to any person under the age of twenty years any such obscene object, as is referred to in IPC Section 292 (definition given below), or offers of attempts so to do, shall be punished (on first conviction with imprisonment or either decription for a term which may extend to three years, and which fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to seven years, and also with fine which may extend to five thousand rupees)"

CASE OF CHENNAI: The cyber crime police arrested Will Heum (56), a Dutch national living in Chennai, for uploading child pornographic materials on the internet. Police recovered his personal computer and pornographic materials from his house.

Heum is already facing a case in a Chengalpattu court for sexually abusing

children of Little Home, an orphanage he

had opened near Mamallapuram. He was arrested in May 2002. Out on bail and living in a rented house in Choolaimedu, he was uploading pictures of children being sexually abused, police said.

This is the **first case of child pornography** to be registered in the country under the IT Act, which came into force on October 27. Heum was booked under Section 67-B of the IT Act, 2008, which deals with digital child pornography, and remanded in judicial custody after being produced before the XI metropolitan magistrate court in Saidapet. The IT Act spells out a maximum punishment of seven years' imprisonment and a fine of Rs 10 lakh.

It was a tip-off from the Child Exploitation Online Protection Centre in Germany through Interpol that led to the arrest of Heum, who has done bit roles in Tamil movies.

Initial inquiries revealed that he had uploaded video clips of foreign children. "We are interrogating him about the source of these clips. We have to verify the seized computer accessories to check if he had uploaded clips of Indian children too," a police officer said.

"It was an example of good co-ordination between the city police and the international agencies. Cyber crime has no geographical barriers,"

Sec. 292,293,294 IPC, Indecent Representation of Women Act

Section 292. Sale, etc., or obscene books, etc.

(1) For the purposes of sub-section (2), a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.]

3(2) Whoever-

(a) Sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever, or

(b) Imports, exports or conveys any obscene object for any of the purposes aforesaid, or knowing or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation, or

(c) Takes part in or receives profits from any business in the course of which he knows or has reason to believe that any such obscene objects are, for any of the purposes aforesaid, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation, or

(d) Advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be procured from or through any person, or

(e) Offers or attempts to do any act which is an offence under this section,

Shall be punished 4[on first conviction with imprisonment of either description for a term which may extend to two years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to five thousand rupees].

5 Exception-This section does not extend to-

(a) Any book, pamphlet, paper, writing, drawing, painting, representation or figure-

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art of learning or other objects of general concern, or

(ii) Which is kept or used bona fide for religious purposes;

(b) Any representation sculptured, engraved, painted or otherwise represented on or in-

(i) Any ancient monument within the meaning or the Ancient Monuments and Archaeological Sites and Remains Act, 1958 (24 of 1958), or

(ii) Any temple, or on any car used for the conveyance of idols, or kept or used for any religious purpose.

Section 292A. **Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail**

Whoever, -

(a) Prints or causes to be printed in any newspaper, periodical or circular, or exhibits or causes to be exhibited, to public view or distributes or causes to be distributed or in any manner puts into circulation any picture or any printed or written document which is grossly indecent, or in scurrilous or intended for blackmail, or

(b) Sells or lets for hire, or for purposes of sale or hire makes, produces or has in his possession, any picture or any printed or written document which is grossly indecent or is scurrilous or intended for blackmail; or

(c) Conveys any picture or any printed or written document which is grossly indecent or is scurrilous or intended for blackmail knowing or having reason to believe that such picture or document will be printed, sold, let for hire distributed or publicly exhibited or in any manner put into circulation; or

(d) Takes part in, or receives profits from, any business in the course of which he knows or has reason to believe that any such newspaper, periodical, circular, picture or other printed or written document is printed, exhibited, distributed, circulated, sold, let for hire, made, produced, kept, conveyed or purchased; or

(e) Advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any Act which is an offence under this section, or that any such newspaper, periodical, circular, picture or other printed or written document which is grossly indecent or is scurrilous or intended for blackmail, can be procured from or through any person; or

(f) Offers or attempts to do any act which is an offence under this section *[shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

Provided that for a second or any subsequent offence under this section, he shall be punished with imprisonment of either description for a term which shall not be less than six months and not more than two years.

Explanation I - For the purposes of this section, the word scurrilous shall be deemed to include any matter which is likely to be injurious to morality or is calculated to injure any person:

Provided that it is not scurrilous to express in good faith anything whatever respecting the conduct of-

(i) A public servant in the discharge of his public functions or respecting his character, so far as his character appears in that conduct and no further; or

(ii) Any person touching any public question, and respecting his character, so far as his character appears in that conduct and no further.

Explanation II - In deciding whether any person has committed an offence under this section, the Court shall have regard inter alia, to the following considerations-

(a) The general character of the person charged, and where relevant the nature of his business;

(b) The general character and dominant effect of the matter alleged to be grossly indecent or scurrilous or intended for blackmail;

(c) Any evidence offered or called by or on behalf of the accused person as to his intention in committing any of the acts specified in this section.

Section 293. **Sale, etc., of obscene objects to young person**

Whoever sells, lets to hire, distributes, exhibits or circulates to any person under the age of twenty years any such obscene object as is referred to in the last preceding section, or offers or attempts so to do, shall be punished 2[on first conviction with imprisonment of either description for a term which may extend to three years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to seven years, and also with fine which may extend to five thousand rupees.

Section 294. **Obscene acts and songs**

Whoever, to the annoyance of others-

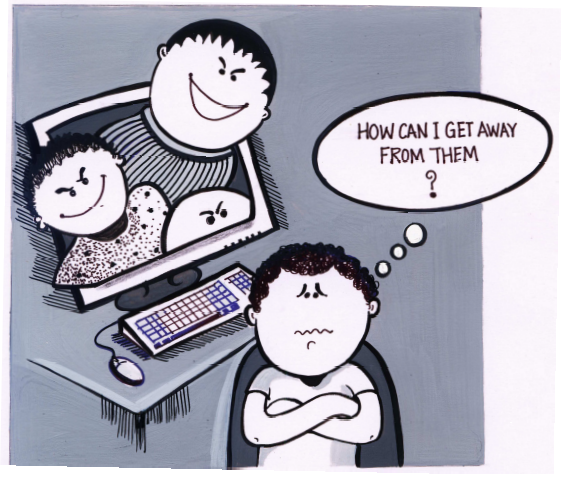
(a) Does any obscene act in any public place, or

(b) Sings, recites or utters any obscene song, balled or words, in or near any public place,

Shall be punished with imprisonment of either description for a term which may extend to three months, or with fine, or with both.

Ch.4.0 CYBER BULLYING

With today's technology bullying has become easier then even the children and youth of this generation do not even need to have personal confrontation. Cyber bullying can be defined as any communication posted or sent by a minor online, by instant messenger, e-mail, Social Networking Site, website, diary site, online profile, interactive game, handheld device, cell phone or other interactive device that is intended to frighten, embarrass, harass or otherwise target another minor.



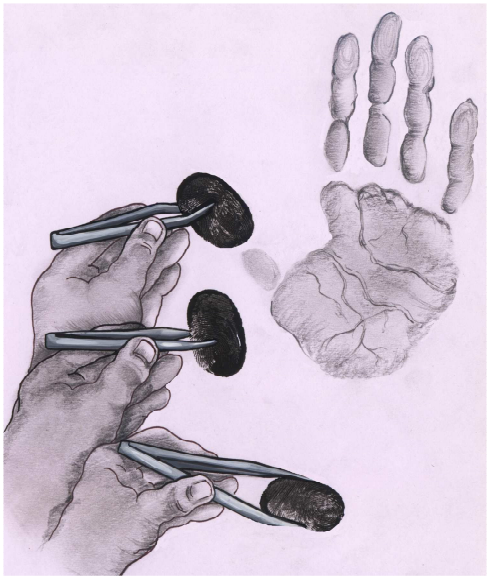
Cyber bullying is disturbingly common among Indian teens. Cyber-Bullying: Our Kids' New Reality is a survey that was conducted from December 2006 – January 2007 by the members of Kids Help Phone that had over 2500 respondents. More than 70 per cent of respondents to the survey reported that they have been bullied online, while 44 per cent said they have bullied someone online. At least 38 percent reported having experienced cyber-bullying within the last three months. Of the methods used, 77 percent reported being bullied by instant messaging, 37 per cent by e-mail and 31 per cent on social networking sites, such as MySpace and Facebook. When bullied online, 43 per cent said they did nothing, 32 per cent confronted the person who bullied them, and 27 per cent told a friend. Although most cyber bullying cases go unreported, police departments take action in trying to prevent it. Because many people are afraid to come to the police about an online problem, the police go to great lengths to find the problems themselves online.

A large number of youth and their parents think that cyber bullying is not a big enough deal to cause problems. However, it has been proven that a victim of this type of bullying can be lead to serious disorders for the future including suicide. When one becomes a victim of cyber bullying, they are a victim for life. Though the bullying itself may go away, the fear, the hurt, and the memories scar the victim forever.

Cyber Bullying is one type of "Unauthorized use" or "Unauthorized access to the facilities". This is "hacking" under Section 66 of ITA 2008 and also liable for compensation under Section 43 of ITA 2008.

Ch. 5.0 IDENTITY THEFT

Identity theft is a term used to refer to fraud that involves stealing money or getting other benefits by pretending to be someone else. The term is relatively new and is actually a misnomer, since it is not inherently possible to steal an identity, only to use it. The person whose identity is used can suffer various consequences when they are held responsible for the perpetrator's actions. At one time the only way for someone to steal somebody else's identity was by killing that person and taking his place. It was typically a violent crime. However, since then, the crime has evolved and today's white collared criminals are a lot less brutal. But the ramifications of an identity theft are still scary.



As per the non-profit Identity Theft Resource Center, identity thefts can be sub-divided into four categories. These are financial identity theft, criminal identity theft, identity cloning, and business/commercial identity theft.

In many cases the victim is not even aware of what is being done till it is already too late. Identity theft may be used to facilitate crimes, including illegal immigration, terrorism, and espionage. It may also be used as a means of blackmail. There have also been cases of identity cloning to attack payment systems, including online credit card processing and medical insurance. Sometimes people may impersonate others for non-financial reasons too. This is often done to receive praise or attention for the victim's achievements. This is sometimes referred to as identity theft in the media, and is a common trend seen by look-a-likes.

One does not have to think too far back before re-collecting a probable victim of identity theft in India.

Illustration 1 : An American national named Ken Haywood, whose most likely fault is, that his Wi-Fi internet connection was hacked, was only recently under the scanner for involvement in the Ahmadabad terrorist attacks. The sad part remains, while speculators and the cyber crime unit suspect foul play and hacking, not once has the term identity theft or identity protection been suggested. And, this just goes to show our current level of awareness towards a threat so obvious.

Illustration 2

Identity Theft

The biggest case of identity theft ever seen, took place in August of 2009. Eleven people, including a US secret service informant, had been charged in connection with the hacking of nine major retailers and the theft and sale of more than 41 million credit and debit card numbers! This data breach is believed to be the largest hacking and identity theft case ever prosecuted by the US Department of Justice, which announced that the suspects were charged with conspiracy, computer intrusion, fraud and identity theft. Three of those charged are US

citizens, while the others are from places such as Estonia, Ukraine, Belarus and China.

The areas of data protection and securitsation are still very weak. How else could 11 people whose nations barely get along, pull of a heist involving a whooping 41 million credit card and debit card numbers. Yes, one can argue that this happened half-way across the globe and India is so much safer. But is it really? Forget the Ken Haywood incident, one might pass it off as an extreme case still in the grey area. But, last year when there was a duplicate Axis bank web page created, which was "phising" for unsuspecting baits on the internet, the victims and crime was a lot closer home.

Illustration 3

Kingfisher Airlines was duped of Rs 17 crore caused by an online ticket booking fraud, caused by credit card bookings. These credit card details were obtained by the thieves from various places like shopping mall, restaurant and petrol-pump employees who swipe these cards, felt the officers working on this case.

"Data loss is a burning issue that should be on the mind of every C-level executive and board member—if it isn't already. Every day we read about companies suffering millions of dollars in losses due to security breaches. Those losses directly hurt the innocent stakeholders of those companies, including hardworking employees and shareholders. Opportunity for data loss is everywhere, and intentional or otherwise, data that ends up in the wrong place can do tremendous harm. It might be at the hands of a single disgruntled employee with a flash drive, or a forgetful member of your finance department leaving a CD-ROM on the subway. But however it happens, data loss can be devastating, and it's only a matter of time before a high-profile company, perhaps a squeaky clean one bursting with integrity and good will, is brought to its knees by a breach" feels Dave DeWalt, McAfee, president and CEO, in MacAfee's and Data monitor's latest research report.

66C Punishment for identity theft. (Inserted Vide ITA 2008)

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with

imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Identity Theft

66D Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

IPC

Section 417A, that prescribes punishment of up to 3 years imprisonment and a fine for cheating, by using any unique identification feature of any other person.

Section 419A, which prescribes punishment of up to 5 years imprisonment and a fine for cheating by impersonation, using a network or computer resource.

Ch.6.0 SALE OF ILLEGAL ARTICLES ON INTERNET

It is becoming increasingly common to find cases where sale of illegal articles such as narcotics drugs, weapons, wildlife etc. is being facilitated by the Internet. Information about the availability of the products for sale is being posted on auction websites, bulletin boards etc.

It is practically impossible to control or prevent a criminal from setting up a website to transact in illegal articles. Additionally, there are several online payment gateways that can transfer money around the world at the click of a button.

The Internet has also created a marketplace for the sale of unapproved drugs, prescription drugs dispensed without a valid prescription, or products marketed with fraudulent health claims.

Many sites focus on selling prescription drugs and are referred to by some as “Internet pharmacies.” These sites offer for sale either approved prescription drug products, or in some cases, unapproved, illegal versions of prescription drugs. This poses a serious potential threat to the health and safety of patients. The broad reach, relative anonymity, and ease of creating new or removing old websites, poses great challenges for law enforcement officials.

As pointed out earlier, the online lottery is the most popular form of internet gambling in India. Most companies marketing and distributing or conducting state government-sponsored lotteries through the internet are not allowed to sell their services in the states that banned lotteries. In most cases, these marketers and distributors limit their online services to consumers who are residents of the states where a lottery is permissible. Notwithstanding the fact there has been no reported case of breach by any company promoting online lotteries, most of these companies (as a safeguard) seek an undertaking from their consumers relating to their residence.

There have been instances where one state has banned the lottery of other states, including online lotteries. In a recent case, the Karnatka High Court upheld the decision of the Karnataka government to make itself a 'lottery free zone' by imposing a ban on lotteries of all other states, including online lotteries under the Lotteries (Regulation) Act 1998. The state government, in this case, directed the closure of the terminals and kiosks selling the online lotteries.

Enforcement over foreign jurisdictions

If the websites are hosted and operated from outside India, it was difficult for the Indian authorities to issue any directive to close them down or prohibit their

access without using its blocking powers under the ITA but under ITA 2008. The authorities have little to worry about, as Indian foreign exchange laws do not permit remittances outside India for gambling related activity, such as the purchase of lottery tickets, football pools and sweepstakes. As a result, a gambling website hosted outside India aiming at receiving money from within India cannot do so through legal channels.

Illustration

Many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'. The clip of the DPS students was kept for selling on the site called Bazee.com by a student from IIT Kharagpur.

case filed under - NDPS Act

Illustration

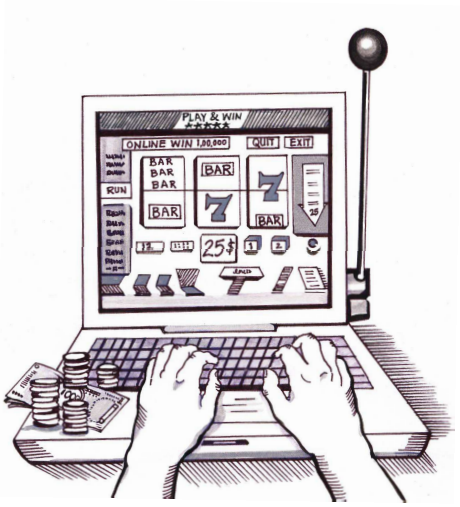
In March 2007, the Pune rural police cracked down on an illegal rave party and arrested hundreds of illegal drug users. The social networking site Orkut.com is believed to be one of the modes of communication for gathering people for the illegal "drug" party.

case is filed under -NDPS Act

Online sale of Arms -**Arms Act will be applicable**

Ch.7.0 ONLINE GAMBLING

There are thousands of Websites that offer online Gambling. The special issue with online gambling is that it is legalised in several countries. So legally the owners of these websites are safe in their home countries. virtual casinos, Cases of money laundering etc are onlne cases.



The legal issues arise when a person residing in a foreign country like India (where such website are illegal) gambles on such a website.

The law related to gambling is also applicable to online gambling. All gambling contracts are considered to be wagering contracts and it is not possible to enforce such contracts under the ICA, detailed above.

Illustration

The website ladbrokes.com permits users to gamble on a variety of sports such as cricket, football, tennis, golf, motor racing, ice hockey, basketball, baseball, darts, snooker, boxing, athletics', rugby, volleyball, motor cycling etc.

Additionally it also features an online casino. The website has no technical measures in place to prohibit residents of certain countries (where online gambling is illegal) from betting at their website

Cyber lotto case: In Andhra

Pradesh one Kola Mohan created a website and an email address on the Internet with the address 'eurolottery@usa.net.' which shows his own name as beneficiary of 12.5 million pound in Euro lottery. After getting confirmation with the email address a telgu newspaper published this as news.

He gathered huge sums from the public as well as from some banks. The fraud came to light only when a cheque amounting Rs 1.73 million discounted by him with Andhra bank got dishonored

The law relating to online gambling in India needs to be understood within the country's socio-cultural context. At the outset, gambling, although not absolutely

prohibited in India, does not receive express encouragement by policy makers. The Indian organized gambling industry is estimated to be worth around US$8

billion. While stringent laws have checked the proliferation of casinos and high street gaming

centres as in many other countries, barring the state of Goa, the lottery business remains the most post popular form of gambling.

Though gambling is not illegal, it is a highly controlled and regulated activity. Modern India is a quasi-federal Constitutional democracy and the powers to legislate are distributed at the federal as well as the state levels. Gambling features in List II of the Constitution of India, this implies that the state governments have the authority to enact laws in order to regulate gambling in the respective states. Thus, there is no single law governing gambling in the entire country. Different states have different laws governing gambling in addition to the laws that have an application across the country. While some states have banned lotteries, other states allow state government lotteries marketed and distributed in other lottery playing and promoting states through private entities.

Regulation of gambling

The courts have defined gambling as 'the payment of a price for a chance to win a prize'. The dominant element of skill or chance shall determine the nature of the game. A game may be deemed to be gambling if the element of chance or luck predominates in deciding its outcome. As a result, Indian courts have held that betting on horse racing and a few card games are not gambling. The right to undertake the business of gambling and lotteries is not considered as a fundamental right protected by the Constitution of India. It may however be pointed out that the state government run lotteries make significant contributions to the state exchequer of several state governments and the Union government, and hence there is a resistance to complete prohibition.

The following legislation is pertinent to gambling:

The Public Gaming Act, 1867

This Act provides punishment for public gambling and for keeping of a 'common gaming house'. This Act also authorises the state governments to enact laws to regulate public gambling in their respective jurisdictions. The penal legislations in respective states have been amended in accordance with their policy on gambling. However, this legislation does not have any direct impact on online gambling unless a wide interpretation is given to the definition of common gaming house so as to include virtual forums as well.

The Indian Contract Act, 1872 (ICA)

The ICA is a codified umbrella legislation that governs all commercial contracts in India. Under the ICA, a wagering contract is the one which cannot be enforced. The Act lays down; 'Agreements by way of wager are void, and no suit shall be brought for recovering anything alleged to be won on any wager or entrusted to

any person to abide by the result of any game or other uncertain event on which any wager is made'. Gambling, lottery and prize games have held to be wagering

contracts and thus void and unenforceable. While a wagering contract is not illegal, it cannot be enforced in a court of law. Thus, the courts will not entertain any cause of action that arises out of a wagering contract.

Lotteries (Regulation) Act, 1998

This Act provides a framework for organizing lotteries in the country. Under this Act, the state governments have been authorized to promote as well as prohibit lotteries within their territorial jurisdiction. This Act also provides for the manner in which the lotteries are to be conducted and prescribes punishment in case of breach of its provision. Lotteries not authorized by the state have been made an offence under the Indian Penal Code. Several non-lottery playing states, like Gujarat and Uttar Pradesh, have prohibited the sale of other state-government lotteries under this Act.

Indian Penal Code, 1860

Section 294A deals with keeping lottery office. It says that whoever keeps any office or place for the purpose of drawing any lottery not being a State lottery or a lottery authorised by the State Government, shall be punished with imprisonment of either description for a term which may extend to six months, or with fine, or with both.

And whoever publishes any proposal to pay any sum, or to deliver any goods, or to do or forbear doing anything for the benefit of any person, on any event or contingency relative or applicable to the drawing of any ticket, lot, number or figure in any such lottery, shall be punished with fine which may extend to one thousand rupees.

Ch.8.0 INTELLECTUAL PROPERTY CRIMES

These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc.

Illustration 1

Bharti Cellular Ltd. filed a case in the Delhi High Court that some cyber squatters had registered domain names such as barticellular.com and bhartimobile.com with Network solutions under different fictitious names. The court directed Network Solutions not to transfer the domain names in question to any third party and the matter is sub-judice.

Illustration 2

Yahoo had sued one Akash Arora for use of the domain name 'Yahooindia.Com' deceptively similar to its 'Yahoo.com'. As this case was governed by the Trade Marks Act, 1958, the additional defence taken against Yahoo's legal action for the interim order was that the Trade Marks Act was applicable only to goods.

Illustration 3

A software professional from Bangalore (India) was booked for stealing the source code of a product being developed by his employers. He started his own company and allegedly used the stolen source code to launch a new software product.

Illustration 4

In 2003, a computer user in China obtained the source code of a popular game - LineageII from an unprotected website. This proprietary code was then sold to several people in 2004. One of those people set up a website, www.l2extreme.com, to offer the "Lineage" game at a discount.

Despite legal warnings from the South Korean company that owned the Lineage source code, the suspect did not shut down the site. He rented powerful servers enough

to accommodate 4,000 simultaneous gamers - and solicited donations from users to help defray the costs.

The loss in potential revenues for the South Korean company was estimated at $750,000 a month. The US FBI arrested the suspect and the website was shut down.

For Piracy - Sec. 51, 63, 63 B Copyright Act will be applicable.

CHAPTER XI : INFRINGEMENT OF COPYRIGHT

51. When copyright infringed

Copyright in a work shall be deemed to be infringed-

(a) when any person, without a licence granted by the owner of the copyright or the Registrar of Copyrights under this Act or in contravention of the conditions of a licence so granted or of any condition imposed by a competent authority under this Act-

(i) does anything, the exclusive right to do which is by this Act conferred upon the owner of the copyright; or

(ii) permits for profit any place to be used for the communication of the work to the public where such communication constitutes an infringement of the copyright in the work, unless he was not aware and had no reasonable ground for believing that such communication to the public would be an infringement of copyright; or

(b) when any person-

(i) makes for sale or hire, or sells or lets for hire, or by way of trade displays or offers for sale or hire, or

(ii) distributes either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright, or

(iii) by way of trade exhibits in public, or

(iv) imports 22[* * *] into India,

any infringing copies of the work:

PROVIDED that nothing in sub-clause (iv) shall apply to the import of one copy of any work for the private and domestic use of the importer.

Explanation: For the purposes of this section, the reproduction of a literary, dramatic, musical or artistic work in the form of a cinematograph film shall be deemed to be an "infringing copy".

63. Offence of infringement of copyright or other rights conferred by this Act

Any person who knowingly infringes or abets the infringement of-

(a) the copyright in a work, or

(b) any other right conferred by this Act, except the right conferred by section 53A,

shall be punishable with imprisonment for a term which shall not be less than six months but which may extend to three years and with fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees:

PROVIDED that where the infringement has not been made for gain in the course of trade or business the court may, for adequate and special reasons to be mentioned in the judgment, impose a sentence of imprisonment for a term of less than six months or a fine of less than fifty thousand rupees.

Explanation: Construction of a building or other structure which infringes or which, if completed, would infringe the copyright in some other work shall not be an offence under this section.

63A. Enhanced penalty on second and subsequent convictions

Whoever having already been convicted of an offence under section 63 is again convicted of any such offence shall be punishable for the second and for every subsequent offence, with imprisonment for a term which shall not be less than one year but which may extend to three years and with fine which shall not be less than one lakh rupees but which may extend to two lakh rupees:

PROVIDED that where the infringement has not been made for gain in the course of trade or business the court may, for adequate and special reasons to be mentioned in the judgement, impose a sentence of imprisonment for a term of less than one year or a fine of less than one lakh rupees:

PROVIDED FURTHER that for the purposes of this section, no cognisance shall be taken of any conviction made before the commencement of the Copyright (Amendment) Act, 1984 (65 of 1984).

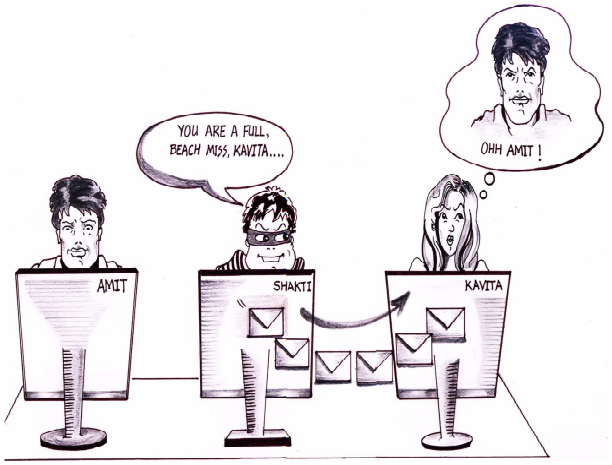
Ch.9.0 EMAIL SPOOFING

A spoofed email is one that appears to originate from one source but actually has been sent from another source e.g steve has an e-mail address steve@cyberlawconsulting.com

Her ex-girlfriend, Sandra spoofs her e-mail and sends obscene messages to all his acquaintances. Since the e-mails appear to have originated from Steve, his friends may take offence and relationships may be spoiled for life.

Forgery of electronic records, Email spoofing Under ITA 2008 Section 66A, 66C.

66A Punishment for sending offensive messages through communication service, etc.(Introduced vide ITAA 2008)



Any person who sends, by means of a computer resource or a communication device,-

a) any **information** that is grossly offensive or has menacing character; or

b) any **information** which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes **by making** use of such computer resource or a communication device,

c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008)

shall be punishable with imprisonment for a term which may extend to two **three** years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

66C Punishment for identity theft. (Inserted Vide ITA 2008)

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Sec 463, 464, 468, 469 IPC

Illustration 1

In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold.

This misinformation was spread by sending spoofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly.

Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money.

Illustration 2

A branch of the erstwhile Global Trust Bank in India experienced a run on the bank. Numerous customers decided to withdraw all their money and close their accounts.

An investigation revealed that someone had sent out spoofed emails to many of the bank's customers stating that the bank was in very bad shape financially and could close operations at any time. The spoofed email appeared to have originated from the bank itself. Unfortunately this information proved to be true in the next few days.

Case of Cyber Extortion and email spoofing

He does not know much about computer hacking, yet 51-year-old cyber criminal Pranab Mitra has stunned even the cyber crime investigation cell of Mumbai police with his bizarre fraud on the Net. Mitra, a former executive of Gujarat Ambuja Cement, was arrested in June 09 for posing as a woman and seducing online an Abu Dhabi-based man,

thereby managing to extort Rs 96 lakh from him. Investigating officer he was remanded to police custody and has been booked for cheating, impersonation, blackmail and extortion under sections 384, 420, 465, 467, 471, 474 of the IPC, read with the newly formed Information Technology Act 2008 66D

66DPunishment for cheating by personation by using computer resource (Inserted Vide ITA 2008)

Whoever, by means of any communication device or

computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Case Story:

Mitra posed as a woman, Rita Basu, and created a fake e-mail ID through which he contacted one V.R. Ninawe. According to the FIR, Mitra trapped Ninawe in a ‘‘cyber-relationship’’ sending emotional messages and indulging in online sex since June 2002.Later, Mitra sent an e-mail that ‘‘she would commit suicide’’ if Ninawe ended the relationship. He also gave him ‘‘another friend Ruchira Sengupta’s’’ e-mail ID which was in fact his second bogus address. When Ninawe mailed at the other ID he was shocked to learn that Mitra had died. Then Mitra began the emotional blackmail by calling up Abu Dhabi to say that police here were searching for Ninawe. Ninawe panicked on hearing the news and asked Mitra to arrange for a good advocate for his defence. Ninawe even deposited a few lakh in the bank as advocate fees. Mitra even sent e-mails as high court and police officials to extort more money. Ninawe finally came down to Mumbai to lodge a police case.

Ch.10.0 FORGERY

Counterfeit currency notes, postage and revenue stamps, mark sheets, academic certificates etc are made by criminals using sophisticated computers, printers and scanners.

IPC Section 463. Forgery.

Whoever makes any false documents or electronic record part of a document or electronic record with, intent to cause damage or injury], to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.

IPC Section 464. Making a false document

A person is said to make a false document or false electronic record-

First - Who dishonestly or fraudulently-

(a) Makes, signs, seals or executes a document or part of a document;

(b) Makes or transmits any electronic record or part of any electronic record;

(c) Affixes any digital signature on any electronic record;

(d) Makes any mark denoting the execution of a document or the authenticity of the digital signature,

With the intention of causing it to be believed that such document or part of document, electronic record or digital signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

Secondly - Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with digital

signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

Thirdly- Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practiced upon him, he does not know the contents of the document or electronic record or the nature of the alterations.

Section 468. Forgery for purpose of cheating

Whoever commits forgery, intending that the 1[document or Electronic Record forged] shall be used for the purpose of cheating, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

Section 469. Forgery for purpose of harming reputation

Whoever commits forgery, 1[intending that the document or Electronic Record forged] shall harm the reputation of any party, or knowing that it is likely to used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

ITA 2008 Section 65. Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation -

For the purposes of this section, "Computer Source Code" means the listing of programmes

Illustration 1

In October 1995, Economic Offences Wing of Crime Branch, Mumbai (India), seized over 22,000 counterfeit share certificates of eight reputed companies worth Rs. 34.47 crores. These were allegedly prepared using Desk Top Publishing Systems.

Illustration 2

Abdul Kareem Telgi, along with several others, was convicted in India on several counts of counterfeiting stamp papers and postage stamps totalling several billion rupees.

Ch.11.0 CYBER DEFAMATION

This occurs when defamation takes place with the help of computers and / or the Internet. e.g. Sameer publishes defamatory matter about Pooja on a website or sends e-mails containing defamatory information to Pooja's friends.

66 A Punishment for sending offensive messages through communication service, etc. (Introduced vide ITAA 2008)

Any person who sends, by means of a computer resource or a communication device,-

a) any **information** that is grossly offensive or has menacing character; or

b) any **information** which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes **by making** use of such computer resource or a communication device,

c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008)

shall be punishable with imprisonment for a term which may extend to **two - three** years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

IPC ,Section 500. Punishment for defamation

Whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both.

IPC ,Section 509. Word, gesture or act intended to insult the modesty of a woman

Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, of that such gesture or object shall be seen, by such woman, or

intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both.

Illustration 1

Abhishek, a teenaged student was arrested by the Thane police in India following a girl's complaint about tarnishing her image in the social networking site Orkut. Abhishek had allegedly created a fake account in the name of the girl with her mobile number posted on the profile.

The profile had been sketched in such a way that it drew lewd comments from many who visited her profile. The Thane Cyber Cell tracked down Abhishek from the false e-mail id that he had created to open up the account.

Illustration 2

The Aurangabad bench of the Bombay high court issued a notice to Google.com following a public interest litigation initiated by a young lawyer.

The lawyer took exception to a community called 'We hate India', owned by someone who identified himself as Miroslav Stankovic. The community featured a picture of the Indian flag being burnt.

Illustration 3

Unidentified persons posted obscene photographs and contact details of a Delhi school girl. Suggestive names like 'sex teacher' were posted on the profile. The matter came to light after the girl's family started receiving vulgar calls referring to Orkut.

Ch.12.0 CYBER STALKING

Cyber stalking refers to the use of the Internet, e-mail, or other electronic communications devices to stalk another person.

Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim's immediate family.

Sec.503 IPC Criminal intimidation

Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation.

Explanation-A threat to inure the reputation of any deceased person in whom the person threatened is interested, is within this section.

2. Sending defamatory messages by email

Sec. 499 IPC Defamation

Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, of defame that person.

Explanation 1 - It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives.

Explanation 2 - It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.

Explanation 3 - An imputation in the form of an alternative or expressed ironically, may amount to defamation.

Explanation 4 - No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgraceful

Illustration 1

Ritu Kohli has the dubious distinction of being the first lady to register the cyber stalking case. A friend of her husband gave her telephonic number in the general chat room. The general chatting facility is provided by some websites like MIRC and ICQ. Where person can easily chat without disclosing his true identity. The friend of husband also encouraged this chatters to speak in slang language to Ms. Kohli. **Section 509 of IPC.**

S. 509 of IPC. Word, gesture or act intended to insult the modesty of a woman - Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both. Sending threatening messages by email. 66A of ITA 2008

Section 66A Punishment for sending offensive messages through communication service, etc.(Introduced vide ITAA 2008)

Any person who sends, by means of a computer resource or a communication device,-

a) Any **information** that is grossly offensive or has menacing character; or

b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes **by making** use of such computer resource or a communication device,

c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008)shall be punishable with imprisonment for a term which may extend to two three years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

Illustration 2

In the first successful prosecution under the California (USA) cyber stalking law, prosecutors obtained a guilty plea from a 50-year-old former security guard who used the Internet to solicit the rape of a woman who rejected his romantic advances. He terrorized the 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized about being raped.

On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her.

Illustration 3

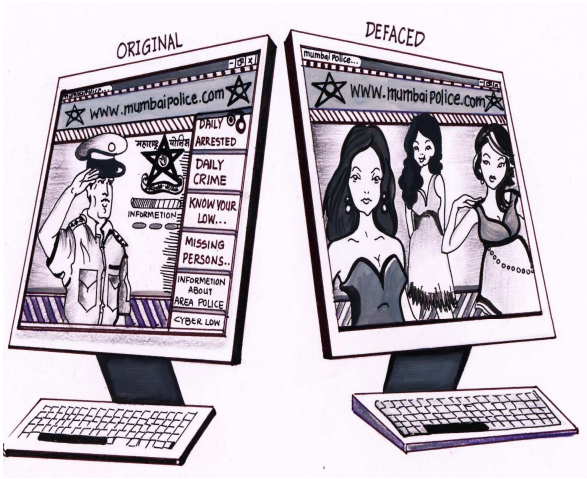
An honors graduate from the University of San Diego in USA terrorized five female university students over the Internet for more than a year. The victims received hundreds of violent and threatening e-mails, sometimes receiving four or five messages a day. The student, who pleaded guilty, told the police that he had committed the crimes because he thought the women were laughing at him and causing others to ridicule him. In reality, the victims had never met him.

Illustration 4

In 2005, a minor from Massachusetts (USA) was convicted in connection with approximately $1 million in victim damages. Over a 15-month period, he had hacked into Internet and telephone service providers, stolen an individual’s personal information and posted it on the Internet, and made bomb threats to many high schools.

Ch.13.0 WEB DEFACEMENT

Website defacement is usually the substitution of the original home page of a website with another page (usually pornographic or defamatory in nature) by a hacker.



Religious and government sites are regularly targeted by hackers in order to display political or religious beliefs. Disturbing images and offensive phrases might be displayed in the process, as well as a signature of sorts, to show who was responsible for the defacement.

Websites are not only defaced for political reasons, many defacers do it just for the thrill. For example, there are online contests in which hackers are awarded points for defacing the largest number of web sites in a specified amount of time. Corporations are also targeted more often than other sites on the Internet and they often seek to take measures to protect themselves from defacement or hacking in general.

Web sites represent the image of a company or organisation and these are therefore especially vulnerable to defacement. Visitors may lose faith in sites that cannot promise security and will become wary of performing online transactions. After defacement, sites have to be shut down for repairs, sometimes for an extended period of time, causing expenses and loss of profit.

Section 463 IPC. Forgery.

1[Whoever makes any false documents or electronic record part of a document or electronic record with, intent to cause damage or injury], to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.

Section 464 IPC. Making a false document

A person is said to make a false document or false electronic record-

First-Who dishonestly or fraudulently-

(a) Makes, signs, seals or executes a document or part of a document;

(b) Makes or transmits any electronic record or part of any electronic record;

(c) Affixes any digital signature on any electronic record;

(d) Makes any mark denoting the execution of a document or the authenticity of the digital signature,

With the intention of causing it to be believed that such document or part of document, electronic record or digital signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

Secondly- Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

Thirdly- Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or electronic record or the nature of the alterations.]

Section 468 IPC. Forgery for purpose of cheating

Whoever commits forgery, intending that the 1[document or Electronic Record forged] shall be used for the purpose of cheating, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

Section 469 IPC. Forgery for purpose of harming reputation

Whoever commits forgery, 1[intending that the document or Electronic Record forged] shall harm the reputation of any party, or knowing that it is likely to used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

Under ITA 2008 Section 65.

Section 65 Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation -

For the purposes of this section, "Computer Source Code" means the listing of programmes, Computer Commands, Design and layout and programme analysis of computer resource in any form.

Illustration 1

Mahesh Mhatre and Anand Khare (alias Dr Neukar) were arrested in 2002 for allegedly defacing the website of the Mumbai Cyber Crime Cell.

They had allegedly used password cracking software to crack the FTP password for the police website. They then replaced the homepage of the website with pornographic content. The duo was also charged with credit card fraud for using 225 credit card numbers, mostly belonging to American citizens.

Illustration 2

In 2001, over 200 Indian websites were hacked into and defaced. The hackers put in words like bugz, death symbol, Paki-king and allahhuakbar.

In the case of 123medicinindia.com, a message was left behind which said – “Catch me if uu can my deraz lazy adminzzz” – challenging the system administrators to trace the miscreants. The offenders were allegedly a group of hackers who go by the name of ‘Pakistani Cyber Warriors’.

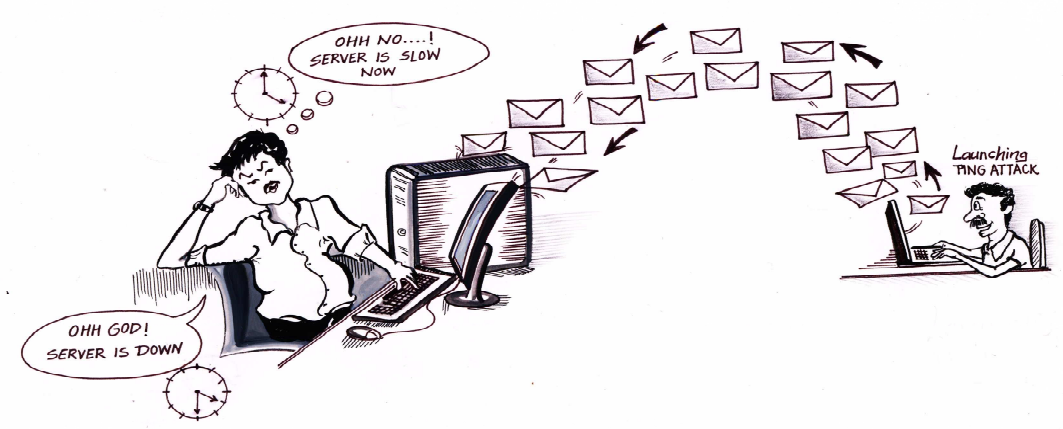
Illustration 3

In 2006, a Turkish hacker using the handle iSKORPiTX was able to breach the security of a group of web servers, containing more than 38,500 web sites in less than a day!

Ch.14.0 EMAIL BOMBING

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

Email bombing is a type of denial-of-service attack. A denial-of-service attack is one in which a flood of information requests is sent to a server, bringing the system to its knees and making the server difficult to access.



Section 66A Punishment for sending offensive messages through communication service, etc.(Introduced vide ITAA 2008)

Any person who sends, by means of a computer resource or a communication device,-

a) Any information that is grossly offensive or has menacing character; or

b) any **information** which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes **by making** use of such computer resource or a communication device,

c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008)

shall be punishable with imprisonment for a term which may extend to two **three** years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or

transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

Illustration 1

A British teenager was cleared of launching a denial-of-service attack against his former employer, in a ruling under the UK Computer Misuse Act.

The teenager was accused of sending 5 million e-mail messages to his ex-employer that caused the company's e-mail server to crash. The judge held that the UK Computer offence.

Illustration 2

In one case, a foreigner who had been residing in Simla, India for almost 30 years wanted to avail of a scheme introduced by the Simla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India.

He decided to take his revenge. Consequently, he sent thousands of mails to the Simla Housing Board and repeatedly kept sending e-mails till their servers crashed.

Ch.15.0 DATA DIDDLING

One of the most common forms of computer crime is data diddling -illegal or unauthorized data alteration. These changes can occur before and during data input or before output. Data diddling cases have affected banks, payrolls, inventory records, credit records, school transcripts and virtually all other forms of data processing known.

Section 66 and 43(d) of the I.T. Act covers the offence of data diddling.

Section 66 Computer Related Offences (Substituted vide ITAA 2008)

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both.

Explanation: For the purpose of this section,-

a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;

b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

Section 43 (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programs residing in such computer, computer system or computer network;

Case in point:

NDMC Electricity Billing Fraud Case: A private contractor who was to deal with receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in his bank who misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance

Illustration 1

The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the New Delhi Municipal Council.

Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional.

He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.

Illustration 2

A keyboard operator processing orders at an Oakland USA department store changed some delivery addresses and diverted several thousand dollars worth of store goods into the hands of accomplices.

Illustration 3

A ticket clerk at the Arizona Veterans' Memorial Coliseum in USA issued full-price basketball tickets, sold them and then, tapping out codes on her computer keyboard, recorded the transactions as half-price sales.

Ch.16.0 SALAMI ATTACKS

These attacks are used for committing financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed.

For instance, a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 2 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month.

The attack is called "salami attack" as it is analogous to slicing the data thinly, like a salami.

Illustration 1

Four executives of a rental-car franchise in Florida USA defrauded at least 47,000 customers using a salami technique.

They modified a computer billing program to add five extra gallons to the actual gas tank capacity of their vehicles. From 1988 through 1991, every customer who returned a car without topping it off ended up paying inflated rates for an inflated total of gasoline.

The thefts ranged from $2 to $15 per customer -difficult for the victims to detect.

Illustration 2

In January 1997, Willis Robinson of Maryland USA, was sentenced to 10 years in prison for "having reprogrammed his Taco Bell drive-up-window cash register - causing it to ring up each $2.99 item internally as a 1-cent item, so that he could pocket $2.98 each time".

The management assumed the error was hardware or software and only caught the perpetrator when he bragged about his crime to coworkers.

Illustration 3

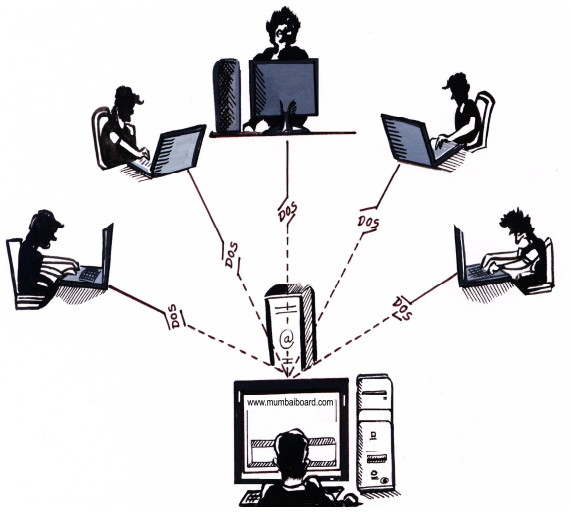
In Los Angeles USA four men were charged with fraud for allegedly installing computer chips in gasoline pumps that cheated consumers by overstating the amounts pumped.

The problem came to light when an increasing number of consumers claimed that they had been sold more gasoline than the capacity of their gas tanks!

However, the fraud was difficult to prove initially because the perpetrators programmed the chips to deliver exactly the right amount of gasoline when asked for five- and 10-gallon amounts (precisely the amounts typically used by inspectors).

Ch.17.0 DENIAL OF SERVICE ATTACK

Denial of Service attacks (DOS attacks) involves flooding a computer with more requests than it can handle. This causes the computer (e.g. a web server) to crash and results in authorized users being unable to access the service offered by the computer.



Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread.

Denial-of-service attacks have had an impressive history having, in the past, blocked out websites like Amazon, CNN, Yahoo and eBay. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the servers crash. Sometimes, many computers are entrenched in this process by installing a Trojan on them; taking control of them and then making them send numerous demands to the targeted computer.

Section 43 of ITA 2008 case will be filled.

43 Penalty and Compensation for damage to computer, computer system, etc (Amended vide ITAA-2008)

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network -

(a) accesses or secures access to such computer, computer system or computer network or computer resource (ITAA2008)

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder,

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means **(Inserted vide ITAA-2008)**

(i) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, (Inserted vide ITAA 2008)

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. (change vide ITAA 2008)

Explanation - for the purposes of this section -

(i) "Computer Contaminant" means any set of computer instructions that are designed -

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "Computer Database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "Computer Virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "Damage" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.

(v) "Computer Source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form (Inserted vide ITAA 2008)

Illustration 1

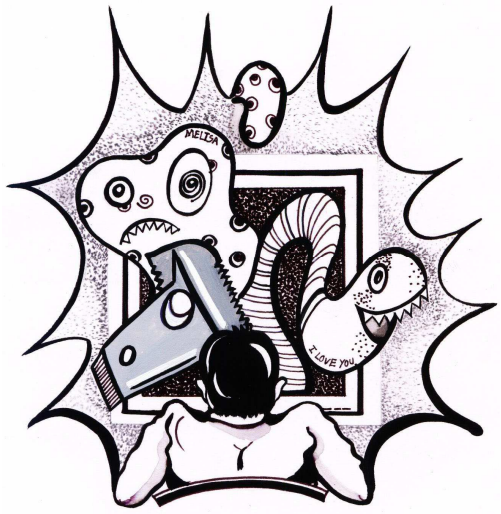
A series of distributed denial of service attacks in February 2000 crippled many popular websites including yahoo.com, amazon.com and cnn.com

Illustration 2

A series of more than 125 separate but coordinated denial of service attacks hit the cyber infrastructure of Estonia in early 2007. The attacks were apparently connected with protests against the Estonian government's decision to remove a Soviet-era war memorial from the capital city. It is suspected that the attacks were carried out by Russian hackers. The attack lasted several days.

Ch.18.0 SPREADING VIRUS / WORM ATTACKS

Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation. A virus might corrupt or delete data on the victim's computer, use the victim's e-mail program to spread itself to other computers, or even erase everything on the victim's hard disk.



Viruses are most easily spread by attachments in e-mail messages or instant messaging messages. Viruses can be disguised as attachments of funny images, greeting cards, or audio and video files. Viruses can also spread through downloads on the Internet. They can be hidden in illicit software or other files or programs.

Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

Brain (in its first incarnation written in January 1986) is considered to be the first computer virus for the PC. The virus is also known as Lahore, Pakistani, Pakistani Brain, Brain-A and UIUC. The virus was written by two brothers, Basit and Amjad Farooq Alvi, who lived in Lahore, Pakistan. The brothers told TIME magazine they had written it to protect their medical software from piracy and was supposed to target copyright infringers only.

The virus came complete with the brothers' address and three phone numbers, and a message that told the user that their machine was infected and for inoculation the user should call them.

When the brothers began to receive a large number of phone calls from people in USA, Britain, and elsewhere, demanding them to disinfect their machines, the brothers were stunned and tried to explain to the outraged callers that their motivation had not been malicious.

They ended up having to get their phone lines cut off and regretted that they had revealed their contact details in the first place. The brothers are still in business in Pakistan as internet service providers in their company called Brain Limited.

Introduces or causes to be introduced any viruses or contaminant in that case, suit filled under Chapter IX of IT Act i.e. Section 43 as a Civil Wrongs under IT Act

Illustration 1

The VBS_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus) was reportedly written by a Filipino undergraduate. In May 2000, this deadly virus became the world's most prevalent virus. Losses incurred during this virus attack were pegged at US $ 10 billion.

VBS_LOVELETTER utilized the addresses in Microsoft Outlook and e-mailed itself to those addresses. The e-mail, which was sent out, had "ILOVEYOU" in its subject line. The attachment file was named "LOVE-LETTER-FOR-YOU.TXT.vbs".

People wary of opening e-mail attachments were conquered by the subject line and those who had some knowledge of viruses, did not notice the tiny .vbs extension and believed the file to be a text file. The message in the e-mail was "kindly check the attached LOVELETTER coming from me".

Illustration 2

Probably the world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. The Internet was, then, still in its developing years and this worm, which affected thousands of computers, almost brought its development to a complete halt. It took a team of experts almost three days to get rid of the worm and in the meantime many of the computers had to be disconnected from the network.

Illustration 3

In 2002, the creator of the Melissa computer virus was convicted. The virus had spread in 1999 and caused more than $80 million in damage by disrupting personal computers, business and government computer networks.

Illustration 4

In 2006, a US citizen was convicted for conspiracy to intentionally cause damage to protected computers and commit computer fraud.

Between 2004 and 2005, he created and operated a malicious software to constantly scan for and infect new computers.

It damaged hundreds of US Department of Defence computers in USA, Germany and Italy. The software compromised computer systems at a Seattle hospital, including patient systems, and damaged more than 1,000 computers in a California school district.

Illustration 5

Logic bombs are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. e.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

Ch.19.0 TROJANS AND KEYLOGGERS

A Trojan, as this program is aptly called, is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

Types of Trojans

The following are the most common types of Trojan:

1. Remote Administration Trojans (RATs) - Modern RATs are very simple to use. They come packaged with two files - the server file and the client file. The hacker tricks someone into running the server file, gets his IP address and gets full control over his/her computer. Some Trojans are limited by their functions, but more functions also mean larger server files. Some Trojans are merely meant for the attacker to use them to upload another Trojan to his target's computer and run it; hence they take very little disk space. Hackers also bind Trojans into other programs, which appear to be legitimate e.g. a RAT could be bound with an egreeting card. There are many programs that detect common Trojans. Firewalls and anti-virus software can be useful in tracing RATs.

2. Password Trojans - Password Trojans search the victim's computer for passwords and then send them to the attacker or the author of the Trojan. Whether it's an Internet password or an email password there is a Trojan for every password. These Trojans usually send the information back to the attacker via Email.

3. Privileges-Elevating Trojans - These Trojans are usually used to fool system administrators. They can either be bound into a common system utility or pretend

to be something harmless and even quite useful and appealing. Once the administrator runs it, the Trojan will give the attacker more privileges on the system. These Trojans can also be sent to less-privileges users and give the attacker access to their account.

4. Destructive Trojans - These Trojans can destroy the victim's entire hard drive, encrypt or just scramble important files. Some might seem like joke programs, while they are actually ripping every file they encounter to pieces.

Some common Trojans

5. Back Orifice (BO) - This Trojan was developed by a community of hackers known as "Cult of the dead cow" (www.cultdeadcow.com). This Trojan can be downloaded from www.BO2K.com and numerous other websites. (Note: the websites keep changing and it is best to use a powerful search engine like www.Google.com to search for the program.)

Back Orifice consists of two parts, a client application and a server application (approximately 122 KB). The client application, running on the hacker's computer, can be used to monitor and control the victim's computer (which runs the server application). The hacker can do the following activities on the victim's computer:

i. Run any program or see any file
ii. Keep a record of all the keys punched on the keyboard
iii. Shutdown or restart the victim's computer
iv. Transfer files to or from the victim computer

The hacker could be in Australia and the victim in China, but still the hacker can do all the above activities on the victim's computer! The following are the main characteristics of BO:

i. BO can only be used on victim computers that are running the Windows 95 or Windows 98 operating systems.

ii. The server part of the program has to be installed on the victim computer. The victim is usually fooled into installing the server part by sending him the Trojan fused with another program (e.g. an electronic Diwali card fused with the Trojan program).
iii. The hacker needs to know the IP address of the victim computer.
iv. If the victim computer is behind a firewall, then BO will not work

6. NetBus - NetBus was developed by a Swedish citizen named Carl-Fredrik Neikter who claimed that he developed it "purely for fun". Netbus can be downloaded from hundreds of websites. It is best to use Google.com to search for the program. Netbus allows the hacker to do numerous activities on the victim's computer. Some of these are:

i. Open/close the CD-ROM once or in intervals (specified in seconds)
ii. Swap mouse buttons - the right mouse button works like the left mouse button and vice versa.
iii. Start any program.
iv. Play any sound-file (it supports only WAV files).
v. Point the mouse to some other place. The hacker can navigate the victim's mouse with his own.
vi. Show a message dialogue on the screen. The answer is sent back to the

hacker. The hacker can ask for the password and the victim would enter it!
vii. Shutdown or log off the victim.
viii. Open any website
ix. Type anything in the program that the victim is using.
x. Obtain a list of all the keys on the keyboard that the victim is punching.
xi. Get an image of the screen (called a screen dump)
xii. Get information about the victim computer.
xiii. Upload any file to the victim computer. Using this feature the hacker can upload any virus or Trojan or update the Netbus Trojan itself.
xiv. Increase and decrease the sound-volume.
xv. Record sounds that the microphone can catch. The sound is sent to the hacker.
xvi. Make click sounds every time a key is pressed.
xvii. Download and delete any file on the victim computer.
xviii. Disable keys on the victim keyboard.

The following are the main characteristics of Netbus:

i. Once it is installed on the victim computer, it runs every time the computer is started184.
ii. Netbus can be used on victim computers that are running the Windows 95 or Windows 98 or Windows NT operating systems

Keyloggers are regularly used were to log all the strokes a victim makes on the keyboard. This assumes sinister proportions, if a key logger is installed on a computer which is regularly used for online banking and other financial transactions. Key-loggers are most commonly found in public computers such as those in cyber cafes, hotels etc. Unsuspecting victims also end up downloading spyware when they click on "friendly" offers for free software.

Illustration 1

A young lady reporter was working on an article about online relationships. The article focused on how people can easily find friendship and even love on the Internet. During the course of her research she made a lot of online friends. One of these 'friends' managed to infect her computer with a Trojan.

This young lady stayed in a small one bedroom apartment and her computer was located in one corner of her bedroom. Unknown to her, the Trojan would activate her web camera and microphone even when the Internet was switched off. A

year later she realized that hundreds of her pictures were posted on pornographic sites around the world!

Illustration 2

The network administrator in a global bank received a beautifully packed CD ROM containing “security updates” from the company that developed the operating system that ran his bank’s servers.

He installed the “updates” which in reality was Trojanized software. 3 years later, the effects were still being felt in the bank’s system!

Internet Time Theft

Ch.20.0 INTERNET TIME THEFT

This connotes the usage by an unauthorized person of the Internet hours paid for by another person.

Illustration

In May 2000, the Delhi police arrested an engineer who had misused the login name and password of a customer whose Internet connection he had set up.

The case was filed under the Indian Penal Code and the Indian Telegraph Act.

Theft of Computer Hardware

Sec. 43 of IT Act 2008 and also under Sec. 378, 379 IPC

Section 43 Penalty and Compensation for damage to computer, computer system, etc (Amended vide ITAA-2008)

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network -

(a) accesses or secures access to such computer, computer system or computer network or computer resource (ITAA2008)

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under,

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

Internet Time Theft

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means **(Inserted vide ITAA-2008)**

(i) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, (Inserted vide ITAA 2008)

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. (change vide ITAA 2008)

Explanation - for the purposes of this section -

(i) "Computer Contaminant" means any set of computer instructions that are designed -

(a) to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "Computer Database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "Computer Virus" means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource;

(iv) "Damage" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.

(v) "Computer Source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form (Inserted vide ITAA 2008)

Section 378. Theft

Whoever intending to take dishonestly any moveable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft.

Internet Time Theft

Explanation1. -A thing so long as it is attached to the earth, not being movable property, is not the subject of theft; but it becomes capable of being the subject of theft as soon as it is severed from the earth.

Explanation 2. -A moving effected by the same act which affects the severance may be a theft.

Explanation 3. -A person is said to cause a thing to move by removing an obstacle which prevented it from moving or by separating it from any other thing, as well as by actually moving it.

Explanation 4. -A person, who by any means causes an animal to move, is said to move that animal, and to move everything which, in consequence of the motion so caused, is moved by that animal.

Explanation 5. -The consent mentioned in the definition may be express or implied, and may be given either by the person in possession, or by any person having for the purpose authority either express or implied.

Section 379. Punishment for theft

Whoever commits theft shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

Web Jacking

Ch.21.0 WEB JACKING

Just as conventional hijacking of an airplane is done by using force, similarly web jacking means forcefully taking over control of a website. The motive is usually the same as hijacking – ransom. The perpetrators have either a monetary or political purpose which they try to satiate by holding the owners of the website to ransom.

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website.

How does web jacking take place?

The administrator of any website has a password and a username that only he (or someone authorized by him) may use to upload files from his computer on the web server (simply put, a server is a powerful computer) where his website is hosted.

Ideally, this password remains secret with the administrator. If a hacker gets hold of this username and password, then he can pretend to be the administrator.

Computers don't recognize people – only usernames and passwords. The web server will grant control of the website to whoever enters the correct password and username combination.

There are many ways in which a hacker may get to know a password, the most common being password cracking wherein a "cracking software" is used to guess a password. Password cracking attacks are most commonly of two types.

The first one is known as the dictionary attack. In this type of attack the software will attempt all the words contained in a predefined dictionary of words.

For example, it may try Rahim, Rahul, Rakesh, Ram, Reema, Reena … in a predefined dictionary of Indian names. These types of dictionaries are readily available on the Internet.

The other form of password cracking is by using 'brute force'. In this kind of attack the software tries to guess the password by trying out all possible combinations of numbers, symbols, letters till the correct password is found. For example, it may try out password combinations like abc123, acbd5679, sdj#%^, weuf*(-)*.

Web Jacking

Some software, available for password cracking using the brute force technique, can check a huge number of password combinations per second.

When compared with a dictionary attack, a brute force attack takes more time, but it is definitely more successful.

Section 65 Of ITA 2008

Section 65 Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation -

For the purposes of this section, "Computer Source Code" means the listing of programs, Computer Commands, Design and layout and program analysis of computer resource in any form.

IPC, Section 383. Extortion

Whoever intentionally puts any person in fear of any injury to that person, or to any other, and thereby dishonestly induces the person so put in fear to deliver to any property or valuable security, or anything signed or sealed which may be converted into a valuable security, commits "extortion".

Illustration

In an incident reported in the USA, the owner of a hobby website for children received an e-mail informing her that a group of hackers had gained control over her website. They demanded a ransom of 1 million dollars from her.

The owner, a schoolteacher, did not take the threat seriously. She felt that it was just a scare tactic and ignored the e-mail.

It was three days later that she came to know, following many telephone calls from all over the country, that the hackers had web jacked her website. Subsequently, they had altered a portion of the website which was entitled ‘How to have fun with goldfish’.

In all the places where it had been mentioned, they had replaced the word ‘goldfish’ with the word ‘piranhas’.

Web Jacking

Piranhas are tiny but extremely dangerous flesh-eating fish. Many children had visited the popular website and had believed what the contents of the website suggested.

These unfortunate children followed the instructions, tried to play with piranhas, which they bought from pet shops, and were very seriously injured.

Ch.22.0 EMAIL FRAUDS

Dear Mr. Justin Williams, I'm Vikas Manjit Singh from Punjab (India). I belong to a city named Ludhiana.

Mr. Williams, I am having a brother in Canada who is also named Justin Williams. He was adopted from my parents by some Mr. William Ram of Welland. Me and my mumy came over to Canada to leave Justin to his new family (William Ram's Family). It happened in June 1985.

So Mr. Justin Williams, if you are the same person I'm talking about. Then please give me some time so that I can let you know the realities.

Imagine the thoughts going through Mr. Justin William's head after reading this email. Is he really adopted? Where are his birth parents? Is this email from his birth brother?

In reality, this is a scam email originating from a college in Sangroor (India)! Canadian citizens are targeted with these emails. If the targets start believing the sender to be their brother, they are asked to send money so that their "brother" can travel to Canada with the proof of the victim's adoption!

This is just one of the hundreds of email scams being perpetrated on the Internet. These scams are commonly referred to as Nigerian 419 scams. These scam emails are believed to originate from Nigeria and section 419 of the Nigerian Penal Code relates to cheating (like the famous section 420 of the Indian Penal Code).

In 2007, conducted a 3 month intensive investigation of hundreds of scam emails. The results were very surprising to say the least. Less than 10% of these emails had actually originated from Nigeria!

A majority of these emails (more than 60%) have originated from Israel, followed by the Netherlands, UK and other European countries. The "birth brother" email was the only one originating from India.

Most of these scam emails promise the receiver millions (or sometimes billions) of dollars. Most commonly the email says that some rich African bureaucrat or businessman or politician has died and left behind a lot of money.

The scamster states that the Government is going to confiscate the money. The only way out is to transfer the money to the bank account of the email recipient. All that the email recipient has to do is send his bank account details. For this a generous fee of a few million dollars will be paid!

If someone actually falls for this scam and provides the bank details, he is sent some official looking documents relating to the bank transfer of a huge sum of money. Once the victim is convinced of the "genuineness" of the transaction, something appears to go wrong.

The victim is informed that a small amount of money (ranging from US$ 100 to 2500) is needed for bank charges or other paper work. This money is the motive behind the elaborate scam. Once the victim pays this money, the scamster disappears from the scene.

The lottery scam emails inform the recipient that he has won a million dollar lottery run by Microsoft, Yahoo or some other well known global company. The winner is asked to provide his bank details and pay a small sum for bank charges and other processing fees.

Another scam email begins with "This is to inform you that we are in possession of a consignment, deposited by British National Lottery which is to be couriered to you". The email asks for 470 pounds to be sent to the courier company so that the cheque for the lottery prize can be sent.

Another scam email comes with the subject line "Blessed is the hand that giveth". The sender claims to be a widow on her deathbed. She wants to donate her wealth to someone who will pray for her.

Another scam email comes from an "employee of the Euro Lottery". The "employee" claims to be in a position to carry out a lottery fraud and is willing to share the money with the email recipient.

What is common in all these scams is that scanned versions of official documents are emailed to potential victims. Once the victim is convinced of the genuineness of the transaction, a small fee is requested for meeting bank charges / legal fees / courier charges etc. It is this small fee that is the motive behind the scam.

It is believed that thousands of people are defrauded of billions of dollars every year through these scams.

Section 420. Cheating and dishonestly inducing delivery of property

Whoever cheats and thereby dishonestly induces the person deceived any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of

either description for a term which may extend to seven years, and shall also be liable to fine.

Criminal breach of trust/Fraud- Sec. 405,406,408,409 IPC

Illustration 1

In 2005, an Indian businessman received an email from the Vice President of a major African bank offering him a lucrative contract in return for a kickback of Rs 1 million.

The businessman had many telephonic conversations with the sender of the email. He also verified the email address of the 'Vice President' from the website of the bank and subsequently transferred the money to the bank account mentioned in the email. It later turned out that the email was a spoofed one and was actually sent by an Indian based in Nigeria.

Illustration 2

A new type of scam e-mail threatens to kill recipients if they do not pay thousands of dollars to the sender, who purports to be a hired assassin.

Replying to the e-mails just sends a signal to senders that they've reached a live account. It also escalates the intimidation.

In one case, a recipient threatened to call authorities. The scammer, who was demanding $20,000, reiterated the threat and sent some personal details about the recipient—address, daughter's full name etc. He gave an ultimatum:

"TELL ME NOW ARE YOU READY TO DO WHAT I SAID OR DO YOU WANT ME TO PROCEED WITH MY JOB? ANSWER YES/NO AND DON'T ASK ANY QUESTIONS!!!"

Some emails claim to be from the FBI in London and inform recipients that an arrest was made in the case.

The e-mail says the recipient's information was found with the suspect and that they should reply to assist in the investigation. These emails are part of the scam!

Ch.23.0 CYBER TERRORISM

Computer crime has hit mankind with unbelievable severity. Computer viruses, worms, Trojans, denial of service attacks, spoofing attacks and e-frauds have taken the real and virtual worlds by storm.

However, all these pale in the face of the most dreaded threat – that of cyber terrorism. has defined cyber terrorism as:

Cyber terrorism is the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.

66F of IT Act 2008

Punishment for cyber terrorism

(1) Whoever,-

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant.

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that

such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

Illustration 1

In 1996, a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a US based Internet Service Provider (ISP) and damaged part of its record keeping system.

The ISP had attempted to stop the hacker from sending out worldwide racist messages under the ISP's name. The hacker signed off with the threat, "you have yet to see true electronic terrorism. This is a promise."

Illustration 2

In 1998, Spanish protestors bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages. E-mail was tied up and undeliverable to the ISP's users, and support lines were tied up with people who couldn't get their mail. The protestors also spammed IGC staff and member accounts, clogged their Web page with bogus credit card orders, and threatened to employ the same tactics against organizations using IGC services.

They demanded that IGC stop hosting the website for the Euskal Herria Journal, a New York-based publication supporting Basque independence.

Protestors said IGC supported terrorism because a section on the Web pages contained materials on the terrorist group ETA, which claimed responsibility for assassinations of Spanish political and security officials, and attacks on military installations. IGC finally relented and pulled the site because of the "mail bombings."

Illustration 3

In 1998, a 12-year-old boy successfully hacked into the controls for the huge Roosevelt Dam on the Salt River in Arizona, USA.

He might have released floodwaters that would have inundated Mesa and Tempe, endangering at least 1 million people.

Illustration 4

In 2005, US security consultants reported that hackers were targeting the U.S. electric power grid and had gained access to U.S. utilities' electronic control systems.

Illustration 5

In 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications." Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems.

Illustration 6

During the Kosovo conflict in 1999, NATO computers were blasted with e-mail bombs and hit with denial-of-service attacks by hacktivists protesting the NATO bombings.

In addition, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according to reports. Web defacements were also common.

Illustration 7

Since December 1997, the Electronic Disturbance Theater (EDT) has been conducting Web sit-ins against various sites in support of the Mexican Zapatistas.

At a designated time, thousands of protestors point their browsers to a target site using software that floods the target with rapid and repeated download requests.

EDT's software has also been used by animal rights groups against organizations said to abuse animals.

Electrohippies, another group of hacktivists, conducted Web sit-ins against the WTO when they met in Seattle in late 1999.

Illustration 8

In 1994, a 16-year-old English boy took down some 100 U.S. defense systems.

Illustration 9

In 1997, 35 computer specialists used hacking tools freely available on 1,900 web sites to shut down large segments of the US power grid. They also silenced the command and control system of the Pacific Command in Honolulu.

Illustration 10

In 2000, was regularly attacked by Distributed Denial of Service attacks by “hactivists” propagating the “right to pornography”. has spearheaded an international campaign against pornography on the Internet.

Illustration 11

In 2001, in the backdrop of the downturn in US-China relationships, the Chinese hackers released the Code Red virus into the wild. This virus infected millions of computers around the world and then used these computers to launch denial of service attacks on US web sites, prominently the web site of the White House.

Illustration 12

In 2001, hackers broke into the U.S. Justice Department's web site and replaced the department's seal with a swastika, dubbed the agency the "United States Department of Injustice" and filled the page with obscene pictures.

Eight New Cyber offences added:

The IT AA, 2008 adds new eight cyber offences viz;

1. sending offensive messages through a computer or mobile phone (Section 66A),
2. receiving stolen computer resource or communication device (Section 66B)
3. Punishment for identity theft (Section 66C)
4. Punishment for cheating by personation using computer resource (Section 66D)
5. Punishment for violating privacy or video voyeurism (Section 66E)
6. Cyber Terrorism (Section 66F)
7. Publishing or transmitting material in electronic form containing sexually explicit act (Section 67A),
8. Child pornography (Section 67B)

Thus, cyber crime police stations have to deal with more cyber crimes. Earlier they were dealing with only two sections, 66 & 67.

Summary of Sections Applicable for Cyber Crimes

Cyber Crime	**ITAA2008 Act Section's**	**IPC Section's**
Email spoofing	66D	416,417,463,465,419
Hacking	66 ,43	378,379,405,406
Web-jacking	65	383
Online sale of narcotics	-	NDPS Act
Virus attacks	43, 66	-
Logic bombs	43, 66	-
Salami attacks	66	-
Denial of Service attacks	43	-
Email bombing	66	-
Pornography & Child Pornography	67 , 67B	292,293,294
Online sale of weapons	-	Arms Act
Bogus websites, cyber frauds	-	420
Forgery of electronic records	-	463, 465, 470, 471
Sending defamatory messages by email	66A	499, 500
Sending threatening messages by email	66A	503, 506
Financial Crime	-	415,384,506,511
Cyber Terrorism	66F	153A, UAPA 15-22
Identity Theft	66C	417A, 419A
Website Defacement	65	463,464,468,469
Data Diddling	65, 43	-

GLOSSARY :

A

AES

The Advanced Encryption Standard that will replace DES (the Data Encryption Standard) around the turn of the century.

ANALOG

The traditional method of modulating radio signals so that they can carry information. Amplitude modulation (AM) and frequency modulation (FM) are the two most common methods of analog modulation. Today, most U.S. cellular systems carry phone conversations using analog; the transition to digital transmissions is happening slowly.

APPLET

Applet is a diminutive form of app (application), and it refers to simple, single-function programs that often ship with a larger product. Programs such as Windows' Calculator, File Manager, and Notepad are examples of applets. It can also refer to little Java programs that run on web pages.

ASCII

American Standard Code for Information Interchange. Bland, unformatted text files are best saved in ASCII (pronounced "askee") format. But ASCII is more than a text file format--it's a standard developed by the American National Standards Institute (ANSI) to define how computers write and read characters. The ASCII set of 128 characters includes letters, numbers, punctuation, and control codes (such as a character that marks the end of a line). Each letter or other character is represented by a number: an uppercase A, for example, is the number 65, and a lowercase z is the number 122. Most operating systems use the ASCII standard, except for Windows NT, which uses the suitably larger and newer Unicode standard.

B

BANDWIDTH

In a general sense, this term describes information-carrying capacity. It can apply to telephone or network wiring as well as system buses, radio frequency signals, and monitors. Bandwidth is most accurately measured in cycles per second, or hertz (Hz), which is the difference between the lowest and highest frequencies transmitted. But it's also common to use bits or bytes per second instead.

C

CACHE

Caches come in many types, but they all work the same way: they store information where you can get to it fast. A Web browser cache stores the pages, graphics, sounds, and URLs of online places you visit on your hard drive; that way, when you go back to the page, everything doesn't have to be downloaded all over again. Since disk access is much faster than Internet access, this speeds things up.

CODEC

As the name implies, codecs are used to encode and decode (or compress and decompress) various types of data--particularly those that would otherwise use up inordinate amounts of disk space, such as sound and video files. See, for example, MP3.

COOKIE

Cookies are small data files written to your hard drive by some Web sites when you view them in your browser. These data files contain information the site can use to track such things as passwords, lists of pages you've visited, and the date when you last looked at a certain page.

CRYPTOGRAPHY

The dividing lines between what is and what is not cryptography have become blurred. But to most people, and for purposes of this class, cryptography is concerned with keeping communications private, i.e. guarding the electronic transfer of your Visa number from peeping Toms on the Internet.

CYBERSQUATTING

Cybersquatting describes the potentially lucrative process of registering popular trademark names or names sufficiently similar to a trademark as Internet domain names, then selling them for outrageous fees to companies who hold the trademarks.

D

DATA MINING

Data mining is the process of discovering new correlations, patterns and trends by sifting through large amounts of data stored in repositories or databases and using pattern recognition technologies as well as statistical and mathematical techniques. Data mining can be a goldmine for any business that wants to improve its bottom line by tracking consumer behavior in new and efficient ways. It is also essential to fields that depend on substantive research, such as healthcare. Along with data mining, however, come privacy concerns: how are miners acquiring their data, i.e.

through cookies, how is it being used, and when does their use of your data put you at risk?

DES

Data Encryption Standard, an encryption method developed by IBM and the U.S. government in the 1970's as an official standard.

DIGITAL CERTIFICATE

In an attempt to assuage fears of online transactions, software vendors, security specialists, and online vendors have developed the concept of digital certificates. A digital certificate is a password-protected file that includes a variety of information: the name and email address of the certificate holder, an encryption key that can be used to verify the digital signature of the holder, the name of the company issuing the certificate, and the period during which the certificate is valid. Certificate authorities (CAs) gather information about a person or company and then issue certificates. These certificates can be used as online identification, much in the same way a driver's license can verify your identity in the physical world.

DIGITAL SIGNATURE

Digital signatures are a means of proving that a file or email message belongs to a specific person, much as a driver's license proves identity in real life. Digital signatures have the added benefit of verifying that your message has not been tampered with. When you sign a message, a hash function--a computation that leaves a specific code, or "digital fingerprint"--is applied to it. If the fingerprint on the recipient's message doesn't match the original fingerprint, the message has been altered.

DOMAIN NAMES

You'll find them to the right of the @ sign in an email address, or about ten characters into a URL. HLS's domain name is law.harvard.edu. See TLDs, Cybersquatting.

E

ENCRYPTION

Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it.

ETHERNET

Ethernet is a standard for connecting computers into a local area network (LAN). The most common form of Ethernet is called 10BaseT, which denotes a peak transmission speed of 10 mbps using copper twisted-pair cable.

F

FILTER

Also known as rules, filters can be used to censor Internet content or to manage incoming and stored mail. Software that supports filters lets you create rules that perform actions, such as preventing a particular Internet user from accessing a prohibited site or automatically routing messages to various folders based on the sender's address. See, for example, PICS.

FIREWALL

If you want to protect any networked server from damage (intentional or otherwise) by those who log in to it, you put up a firewall. This could be a dedicated computer equipped with security measures such as a dial-back feature, or it could be software-based protection called defensive coding.

H

HASH

A hash function takes a variable sized input and has a fixed size output. What this means in plain English is that the hash is used to authenticate an email or document by leaving a specific piece of code on it, such that the document has a "digital fingerprint" that would signal tampering.

HTML

Hypertext Markup Language. As its name suggests, HTML is a collection of formatting commands that create hypertext documents--Web pages, to be exact. When you point your Web browser to a URL, the browser interprets the HTML commands embedded in the page and uses them to format the page's text and graphic elements. HTML commands cover many types of text formatting (bold and italic text, lists, headline fonts in various sizes, and so on), and also have the ability to include graphics and other nontext elements.

I

IP ADDRESS

This address is a unique string of numbers that identifies a computer on the Internet. These numbers are usually shown in groups separated by periods, like this: 123.123.23.2. All resources on the Internet must have an IP address--or else they're not on the Internet at all.

ISDN

Integrated Services Digital Network. The plain old telephone system doesn't handle large quantities of data, and the phone companies realized this a long time ago. So the ISDN spec was hammered out in 1984 to allow for wide-bandwidth digital transmission using the public switched telephone network. Under ISDN, a phone call can transfer 64 kilobits of digital data per second. But it's not always easy to adopt.

ISP

Internet Service Provider. Once upon a time, you could only connect to the Internet if you belonged to a major university or had a note from the Pentagon. Not anymore: ISPs have arrived to act as your (ideally) user-friendly front end to all that the Internet offers. Most ISPs have a network of servers (mail, news, Web, and the like), routers, and modems attached to a permanent, high-speed Internet "backbone" connection. Subscribers can then dial into the local network to gain Internet access--without having to maintain servers, file for domain names, or learn Unix.

J

JAVA

Sun Microsystems' Java is a programming language for adding animation and other action to Web sites. The small applications (called applets) that Java creates can play back on any graphical system that's Web-ready, but your Web browser has to be Java-capable for you to see it.

K

KEY

Used widely in cryptography, keys are like pieces of code that allow you to encrypt and decrypt data. Incidentally, a key can be used to perform other mathematical operations as well.

L

LAN

Local area network. A local area network is a short-distance network used to link a group of computers together within a building. 10BaseT Ethernet is the most commonly used form of LAN. A piece of hardware called a hub serves as the common wiring point, enabling data to be sent from one machine to another over the network. LANs are typically limited to distances of less than 500 meters and provide low-cost, high-bandwidth networking capabilities within a small geographical area.

M

META TAG

These pieces of HTML are embedded into the heading sections of an HTML web page and are invisible to surfers. They are designed to help classify a web page for search engines, etc. but are now used to stuff lots of terms into a web page that may make it more visible to a web surfer. For example, we could stuff our IS99 web page with invisible and irrelevant meta tags such as "Bill Clinton" so that whenever a person does a search on Bill Clinton, our page will come up in the search results.

MP3

MPEG-1, Layer 3. MP3 is a codec that compresses standard audio tracks into much smaller sizes without significantly compromising sound quality. The rise of MP3 has generated a highly publicized debate concerning the distribution and protection of music over the Internet.

MPEG

Moving Pictures Experts Group. MPEG is a standard for compressing sound and movie files into an attractive format for downloading--or even streaming--across the Internet. The MPEG-1 standard streams video and sound data at 150 kilobytes per second--the same rate as a single-speed CD-ROM drive--which it manages by taking key frames of video and filling only the areas that change between the frames. Unfortunately, MPEG-1 produces only adequate quality video, far below that of standard TV. MPEG-2 compression improves things dramatically. With MPEG-2, a properly compressed video can be shown at near-laserdisc clarity with a CD-quality stereo soundtrack. For that reason, modern video delivery mediums, such as digital satellite services and DVD, use MPEG-2.

N

NETIZEN

Citizens of the Internet. If you were not a netizen by this fall, you will certainly become one during this course.

P

P3P

Platform for Privacy Preference Project. The P3P project, activity, products, and specifications seek to enable Web sites to express their privacy practices and enable users to exercise preferences over those practices. P3P products will act as an initial privacy-screening device and attempt to address the current privacy concerns that plague both Internet surfers and webmasters. Users will be informed of site practices, will be able to

delegate decisions to their computer when appropriate, and will be able to tailor their relationship to specific sites vis a vis privacy preferences.

PICS

Platform for Internet Content Selection. PICS is a filtering scheme that allows content providers and independent organizations to publish their own content-based label for any URL. Both content providers and third party users may choose which rating system to use.

PROTOCOL

Computers can't just throw data at each other any old way. Because so many different types of computers and operating systems connect via modems or other connections, they have to follow communications rules called protocols. The Internet is a very heterogenous collection of networked computers and is full of protocols.

PROXY SERVER

A proxy server is a system that caches items from other servers to speed up access. On the Web, a proxy first attempts to find data locally, and if it's not there, fetches it from the remote server where the data resides permanently.

PUBLIC KEY CRYPTOGRAPHY

In public key cryptography, each person gets a pair of keys, one called the public key and the other called the private key. The public key is published, while the private key is kept secret. There is no need for the sender and receiver to share secret information; all communications involve only public keys, and no private key is ever transmitted or shared. See Secret Key Cryptography. Therefore, you don't have to worry about whether the communications channels transmitting your encrypted message are sufficiently secure. The only requirement is that public keys be associated with their users in a trusted (authenticated) manner. Anyone can send a confidential message by just using public information, but the message can only be decrypted with a private key, which is in the sole possession of the intended recipient.

S

SDMI

Secure Digital Music Initiative. An attempt to create an alternative to MP3 that would allow companies to track copyrights and be secure in the knowledge that a user could not remove that copyright information. See sdmi.org.

SECRET KEY CRYPTOGRAPHY

Secret key is the traditional method of encryption and decryption. In secret key, or "symmetric key", the sender and receiver of a message know and use the same secret key: the sender uses the secret key to encrypt the message, and the receiver uses the same secret key to decrypt the message. The main challenge, however, is getting the sender and receiver to agree on the secret key without anyone else finding out. Because all keys in a secret key system must remain secret, secret-key cryptography often has difficulty providing secure key management, especially in open systems with a large number of users. See public key cryptography.

SERVER

The business end of a client/server setup, a server is usually a computer that provides the information, files, Web pages, and other services to the client that logs on to it. (The word server is also used to describe the software and operating system designed to run server hardware.) The client/server setup is analogous to a restaurant with waiters and customers. Some Internet servers take this analogy to extremes and become inattentive, or even refuse to serve you.

SPAM

Spiced Ham. Hormel's famous can o' additives has given its name to something almost as disgusting: junk email. Spam can be a mass mailing to bulletin boards, newsgroups, or lists of people. But spam is never welcome: if you spam or get spammed, flame wars can ensue.

SPIDER

Also known as a Web spider, this class of robot software explores the World Wide Web by retrieving a document and following all the hyperlinks in it. Web sites tend to be so well linked that a spider can cover vast amounts of the Internet by starting from just a few sites. After following the links, spiders generate catalogs that can be accessed by search engines. Popular search sites like Alta Vista, Excite, and Lycos use this method.

STREAMING

Data is streaming when it's moving quickly from one chunk of hardware to another and doesn't have to be all in one place for the destination device to do something with it. When your hard disk's data is being written to a tape backup device, it's streaming. When you're watching a QuickTime movie on the Internet, it's not streaming, because the movie must be fully downloaded before you can play it.

T

TLDs

Top Level Domains. TLDs refer to the last extension on a domain name , like. "edu" or "com" or "mil". In a hierarchical classification system, TLD's fill the highest, or most generalized, level of classification; currently, there are about 260 of them (most of them country extensions like .uk or .fr). Their future -- particularly who owns the right to assign and create new TLDs -- is the subject of much contention and, not surprisingly, our first two classes.

U

UNIX

Unix took off in the early 1970s as a general-purpose operating system. Since much of the Internet is hosted on Unix machines, the operating system took on a new surge of popularity in the early 1990s. Unix comes in many flavors--including Xenix, Ultrix, GNU, and Linux--and runs on a variety of platforms, which makes its development a subject of widespread discussion.

USENET

Usenet is a worldwide network of thousands of unix systems with a decentralized administration. The Usenet systems exist to transmit postings to special-interest newsgroups covering just about any topic you can imagine (and many you wouldn't even want to imagine).

W

WARES

Wares is short for software or hardware.

WIPO

The World Intellectual Property Organization, located in Geneva, Switzerland.